Military Health System (MHS)
DITSCAP Checklist

Requirement	Description	Information Assurance Service
1.0 Security Design and Configuration		
1.1 Procedural Review	An annual IA review is conducted that comprehensively evaluates existing policies and processes to ensure procedural consistency and to ensure that they fully support the goal of uninterrupted operations. (**Ref:** DoDI 8500.2, February 6, 2003)	**Availability**
1.2 Best Security Practices	The DoD information system security design incorporates best security practices such as single sign-on, PKE, smart card, and biometrics. (**Ref:** DoDI 8500.2, February 6, 2003)	**Integrity**
1.3 Control Board	All DoD information systems are under the control of a chartered configuration control board that meets regularly. (**Ref:** DoDI 8500.2, February 6, 2003)	**Integrity**
1.4 Configuration Specifications	A DoD reference document, such as a security technical implementation guide or security recommendation guide constitutes the primary source for security configuration or implementation guidance for the deployment of newly acquired IA- and IA-enabled IT products that require use of the product's IA capabilities. If a DoD reference document is not available, the following are acceptable in descending order as available: (1) Commercially accepted practices (e.g., SANS); (2) Independent testing results (e.g., ICSA); or (3) Vendor literature. (**Ref:** DoDI 8500.2, February 6, 2003)	**Integrity**
1.5 Compliance Testing	A comprehensive set of procedures is implemented that tests all patches, upgrades, and new AIS applications prior to deployment. (**Ref**: DoDI 8500.2, February 6, 2003)	**Availability**
1.6 Dedicated IA Services	Acquisition or outsourcing of dedicated IA services, such as incident monitoring, analysis and response; operation of IA devices, such as firewalls; or key management services are supported by a formal risk analysis and approved by the DoD Component CIO. (**Ref:** DoDI 8500.2, February 6, 2003)	**Integrity**
1.7 Functional Architecture for AIS Applications	For AIS applications, a functional architecture that identifies the following has been developed and is maintained: - all external interfaces, the information being exchanged, and the protection mechanisms associated with each interface; - user roles required for access control and the access privileges assigned to each role; - unique security requirements (e.g., encryption of key data elements at rest); - categories of sensitive information processed or stored by the AIS application, and their specific protection plans (e.g., Privacy Act, HIPAA); - restoration priority of subsystems, processes, or information. (**Ref:** DoDI 8500.2, February 6, 2003)	**Integrity**

Military Health System (MHS)
DITSCAP Checklist

Requirement	Description	Information Assurance Service
1.8 Hardware (HW) Baseline	A current and comprehensive baseline inventory of all hardware (HW) (to include manufacturer, type, model, physical location and network topology or architecture) required to support enclave operations is maintained by the Configuration Control Board (CCB) and as part of the SSAA. A backup copy of the inventory is stored in a fire-rated container or otherwise not collocated with the original. (**Ref:** DoDI 8500.2, February 6, 2003)	**Availability**
1.9 Interconnection Documentation	For AIS applications, a list of all [potential] hosting enclaves is developed and maintained along with evidence of deployment planning and coordination and the exchange of connection rules and requirements. For enclaves, a list of all hosted AIS applications, interconnected outsourced IT-based processes, and interconnected IT platforms is developed and maintained along with evidence of deployment planning and coordination and the exchange of connection rules and requirements. (**Ref:** DoDI 8500.2, February 6, 2003)	**Integrity**
1.10 IA Impact Assessment	Changes to the DoD information system are assessed for IA and accreditation impact prior to implementation. (**Ref:** DoDI 8500.2, February 6, 2003)	**Integrity**
1.11 IA for IT Services	Acquisition or outsourcing of IT services explicitly addresses Government, service provider, and end user IA roles and responsibilities. (**Ref:** DoDI 8500.2, February 6, 2003)	**Integrity**
1.12 Mobile Code	The acquisition, development, and/or use of mobile code to be deployed in DoD systems meets the following requirements **{1 - 7 below}**: (**Ref:** DODI 8500.2, February 6, 2003)	**Integrity**
	(1) Emerging mobile code technologies that have not undergone a risk assessment by NSA and been assigned to a Risk Category by the DoD CIO is not used. (**Ref:** DoDI 8500.2, February 6, 2003)	**Integrity**
	(2) Category 1 mobile code is signed with a DoD-approved PKI code signing certificate; use of unsigned Category 1 mobile code is prohibited; use of Category 1 mobile code technologies that cannot block or disable unsigned mobile code (e.g., Windows Scripting Host) is prohibited. (**Ref:** DoDI 8500.2, February 6, 2003)	**Integrity**

Requirement	Description	Information Assurance Service
	(3) Category 2 mobile code which executes in a constrained environment without access to system resources (e.g., Windows registry, file system, system parameters, network connections to other than the originating host) may be used. (**Ref:** DoDI 8500.2, February 6, 2003)	**Integrity**
	(4) Category 2 mobile code that does not execute in a constrained environment may be used when obtained from a trusted source over an assured channel (e.g., SIPRNET, SSL connection, S/MIME, code is signed with a DoD-approved code signing certificate). (**Ref:** DoDI 8500.2, February 6, 2003)	**Integrity**
	(5) Category 3 mobile code may be used. (**Ref:** DoDI 8500.2, February 6, 2003)	**Integrity**
	(6) All DoD workstation and host software are configured, to the extent possible, to prevent the download and execution of mobile code that is prohibited. (**Ref:** DoDI 8500.2, February 6, 2003)	**Integrity**
	(7) The automatic execution of all mobile code in email is prohibited; email software is configured to prompt the user prior to executing mobile code in attachments. (**Ref:** DoDI 8500.2, February 6, 2003)	**Integrity**
1.13 Non-repudiation	NIST FIPS 140-2 validated cryptography (e.g., DoD PKI class 3 or 4 token) is used to implement encryption (e.g., AES, 3DES, DES, Skipjack), key exchange (e.g., FIPS 171), digital signature (e.g., DSA, RSA, ECDSA), and hash (e.g., SHA-1, SHA-256, SHA-384, SHA-512). Newer standards should be applied as they become available. (**Ref:** DoDI 8500.2, February 6, 2003)	**Integrity**
1.14 Public Domain Software Controls	Binary or machine executable public domain software products and other software products with limited or no warranty such as those commonly known as freeware or shareware are not used in DoD information systems unless they are necessary for mission accomplishment and there are no alternative IT solutions available. Such products are assessed for information assurance impacts, and approved for use by the DAA. The assessment addresses the fact that such software products are difficult or impossible to review, repair, or extend, given that the Government does not have access to the original source code and there is no owner who could make such repairs on behalf of the Government. (**Ref:** DoDI 8500.2, February 6, 2003)	**Availability**

Military Health System (MHS)
DITSCAP Checklist

Requirement	Description	Information Assurance Service
1.15 Ports, Protocols, and Services	DoD information systems comply with DoD ports, protocols, and services guidance. AIS applications, outsourced IT-based processes and platform IT identify the network ports, protocols, and services they plan to use as early in the life cycle as possible and notify hosting enclaves. Enclaves register all active ports, protocols, and services in accordance with DoD and DoD Component guidance. (**Ref:** DoDI 8500.2, February 6, 2003)	**Availability**
1.16 Configuration Management Process	A configuration management (CM) process is implemented that includes requirements for: (1) Formally documented CM roles, responsibilities, and procedures to include the management of IA information and documentation; (2) A configuration control board that implements procedures to ensure a security review and approval of all proposed DoD information system changes, to include interconnections to other DoD information systems; (3) a testing process to verify proposed configuration changes prior to implementation in the operational environment; and (4) A verification process to provide additional assurance that the CM process is working effectively and that changes outside the CM process are technically or procedurally not permitted. (**Ref:** DoDI 8500.2, February 6, 2003)	**Integrity**
1.17 Information Assurance Documentation	All appointments to required IA roles (e.g., DAA and Information Assurance Manager/Information Assurance Officer) are established in writing, to include assigned duties and appointment criteria such as training, security clearance, and IT-designation. A System Security Plan is established that describes the technical, administrative, and procedural IA program and policies that govern the DoD information system, and identifies all IA personnel and specific IA requirements and objectives (e.g., requirements for data handling or dissemination, system redundancy and backup, or emergency response). (**Ref:** DoDI 8500.2, February 6, 2003)	**Availability**
1.18 System Library Management Controls	System libraries are managed and maintained to protect privileged programs and to prevent or minimize the introduction of unauthorized code. (**Ref:** DoDI 8500.2, February 6, 2003)	**Integrity**
1.19 Software Quality	Software quality requirements and validation methods that are focused on the minimization of flawed or malformed software that can negatively impact integrity or availability (e.g., buffer overruns) are specified for all software development initiatives. (**Ref:** DoDI 8500.2, February 6, 2003)	**Integrity**

Requirement	Description	Information Assurance Service
1.20 System State Changes	System initialization, shutdown, and aborts are configured to ensure that the system remains in a secure state. (**Ref:** DoDI 8500.2, February 6, 2003)	**Integrity**
1.21 Software (SW) Baseline	A current and comprehensive baseline inventory of all software (SW) (to include manufacturer, type, and version and installation manuals and procedures) required to support DoD information system operations is maintained by the CCB and as part of the C&A documentation. A backup copy of the inventory is stored in a fire-rated container or otherwise not collocated with the original. (**Ref:** DoDI 8500.2, February 6, 2003)	**Availability**
1.22 Acquisition Standards	The acquisition of all IA- and IA-enabled GOTS IT products is limited to products that have been evaluated by the NSA or in accordance with NSA-approved processes. The acquisition of all IA- and IA-enabled COTS IT products is limited to products that have been evaluated or validated through one of the following sources - the International Common Criteria (CC) for Information Security Technology Evaluation Mutual Recognition Arrangement, the NIAP Evaluation and Validation Program, or the FIPS validation program. Robustness requirements, the mission, and customer needs will enable an experienced information systems security engineer to recommend a Protection Profile, a particular evaluated product or a security target with the appropriate assurance requirements for a product to be submitted for evaluation (See also DCSR-1). (**Ref:** DoDI 8500.2, February 6, 2003)	**Confidentiality**
1.23 Specified Robustness - Medium	At a minimum, medium-robustness COTS IA and IA-enabled products are used to protect sensitive information when the information transits public networks or the system handling the information is accessible by individuals who are not authorized to access the information on the system. The medium-robustness requirements for products are defined in the Protection Profile Consistency Guidance for Medium Robustness published under the IATF. COTS IA and IA-enabled IT products used for access control, data separation, or privacy on sensitive systems already protected by approved medium-robustness products, at a minimum, satisfy the requirements for basic robustness. If these COTS IA and IA-enabled IT products are used to protect National Security Information by cryptographic means, NSA-approved key management may be required. (**Ref:** DoDI 8500.2, February 6, 2003)	**Confidentiality**
2.0 Identification and Authentication		

Requirement	Description	Information Assurance Service
2.1 Key Management	Symmetric Keys are produced, controlled, and distributed using NIST-approved key management technology and processes. Asymmetric Keys are produced, controlled, and distributed using DoD PKI Class 3 certificates or pre-placed keying material. (**Ref:** DoDI 8500.2, February 6, 2003)	**Integrity**
2.2 Token and Certificate Standards	Identification and authentication is accomplished using the DoD PKI Class 3 certificate and hardware security token (when available). (**Ref:** DoDI 8500.2, February 6, 2003)	**Integrity**
2.3 Group Identification and Authentication	Group authenticators for application or network access may be used only in conjunction with an individual authenticator. Any use of group authenticators not based on the DoD PKI has been explicitly approved by the Designated Approving Authority (DAA). (**Ref:** DoDI 8500.2, February 6, 2003)	**Confidentiality**
2.4 Individual Identification and Authentication	DoD information system access is gained through the presentation of an individual identifier (e.g., a unique token or user login ID) and password. For systems utilizing a logon ID as the individual identifier, passwords are, at a minimum, a case sensitive 8-character mix of upper case letters, lower case letters, numbers, and special characters, including at least one of each (e.g., emPagd2!). At least four characters must be changed when a new password is created. Deployed/tactical systems with limited data input capabilities implement the password to the extent possible. Registration to receive a user ID and password includes authorization by a supervisor, and is done in person before a designated registration authority. (**Ref:** DoDI 8500.2, February 6, 2003)	**Confidentiality**
	Additionally, to the extent system capabilities permit, system mechanisms are implemented to enforce automatic expiration of passwords and to prevent password reuse. All factory set, default or standard-user IDs and passwords are removed or changed. Authenticators are protected commensurate with the classification or sensitivity of the information accessed; they are not shared; and they are not embedded in access scripts or stored on function keys. Passwords are encrypted both for storage and for transmission. (**Ref:** DoDI 8500.2, February 6, 2003)	**Confidentiality**
3.0 Enclave and Computing Environment		
3.1 Audit Trail, Monitoring, Analysis and Reporting	Audit trail records from all available sources are regularly reviewed for indications of inappropriate or unusual activity. Suspected violations of IA policies are analyzed and reported in accordance with DoD information system IA procedures. (**Ref:** DoDI 8500.2, February 6, 2003)	**Integrity**

Military Health System (MHS)
DITSCAP Checklist

Requirement	Description	Information Assurance Service
3.2 Changes to Data	Access control mechanisms exist to ensure that data is accessed and changed only by authorized personnel. (**Ref:** DoDI 8500.2, February 6, 2003)	**Integrity**
3.3 Instant Messaging	Instant messaging traffic to and from instant messaging clients that are independently configured by end users and that interact with a public service provider is prohibited within DoD information systems. Both inbound and outbound public service instant messaging traffic is blocked at the enclave boundary. Note: This does not include IM services that are configured by a DoD AIS application or enclave to perform an authorized and official function. (**Ref:** DoDI 8500.2, February 6, 2003)	**Integrity**
3.4 Network Device Controls	An effective network device (e.g., routers, switches, firewalls) control program is implemented and includes: instructions for restart and recovery procedures; restrictions on source code access, system utility access, and system documentation; protection from deletion of system and application files, and a structured process for implementation of directed solutions (e.g., IAVA). (**Ref:** DoDI 8500.2, February 6, 2003)	**Integrity**
3.5 Privileged Account Control	All privileged user accounts are established and administered in accordance with a role-based access scheme that organizes all system and network privileges into roles (e.g., key management, network, system administration, database administration, web administration). The IAM tracks privileged role assignments. (**Ref:** DoDI 8500.2, February 6, 2003)	**Integrity**
3.6 Production Code Change Controls	Application programmer privileges to change production code and data are limited and are periodically reviewed. (**Ref:** DoDI 8500.2, February 6, 2003)	**Integrity**
3.7 Audit Reduction and Report Generation	Tools are available for the review of audit records and for report generation from audit records. (**Ref**: DoDI 8500.2, February 6, 2003)	**Integrity**
3.8 Security Configuration Compliance	For Enclaves and AIS applications, all DoD security configuration or implementation guides have been applied. (**Ref:** DoDI 8500.2, February 6, 2003)	**Availability**
3.9 Software Development Change Controls	Change controls for software development are in place to prevent unauthorized programs or modifications to programs from being implemented. (**Ref:** DoDI 8500.2, February 6, 2003)	**Integrity**
3.10 Transmission Integrity Controls	Good engineering practices with regards to the integrity mechanisms of COTS, GOTS and custom developed solutions are implemented for incoming and outgoing files, such as parity checks and cyclic redundancy checks (CRCs). (**Ref:** DoDI 8500.2, February 6, 2003)	**Integrity**

Military Health System (MHS)
DITSCAP Checklist

Requirement	Description	Information Assurance Service
3.11 Audit Trail Protection	The contents of audit trails are protected against unauthorized access, modification, or deletion. (**Ref:** DoDI 8500.2, February 6, 2003)	**Integrity**
3.12 Voice over Internet Protocol	Voice over Internet Protocol (VoIP) traffic to and from workstation IP telephony clients that are independently configured by end users for personal use is prohibited within DoD information systems. Both inbound and outbound individually configured voice over IP traffic is blocked at the enclave boundary. Note: This does not include VoIP services that are configured by a DoD AIS application or enclave to perform an authorized and official function. (**Ref:** DoDI 8500.2, February 6, 2003)	**Availability**
3.13 Virus Protection	All servers, workstations, and mobile computing devices implement virus protection that includes a capability for automatic updates. (**Ref:** DoDI 8500.2, February 6, 2003)	**Availability**
3.14 Wireless Computing and Networking	Wireless computing and networking capabilities from workstations, laptops, personal digital assistants (PDAs), handheld computers, cellular phones, or other portable electronic devices are implemented in accordance with DoD wireless policy, as issued. Unused wireless computing capabilities internally embedded in interconnected DoD IT assets are normally disabled by changing factory defaults, settings or configurations prior to issue to end users. Wireless computing and networking capabilities are not independently configured by end users. (**Ref:** DoDI 8500.2, February 6, 2003)	**Availability**
3.15 Affiliation Display	To help prevent inadvertent disclosure of controlled information, all contractors are identified by the inclusion of the abbreviation "ctr" and all foreign nationals are identified by the inclusion of their two-character country code in: - DoD user e-mail addresses (e.g., john.smith.ctr@army.mil or john.smith.uk@army.mil); - DoD user e-mail display names (e.g., John Smith, Contractor<john.smith.ctr@army.mil> or John Smith, United Kingdom <john.smith.uk@army.mil>); and - automated signature blocks (e.g., John Smith, Contractor, J-6K, Joint Staff or John Doe, Australia, LNO, Combatant Command). Contractors who are also foreign nationals are identified as both (e.g., john.smith.ctr.uk@army.mil). Country codes and guidance regarding their use are in FIPS 10-4. (**Ref:** DoDI 8500.2, February 6, 2003)	**Confidentiality**

Military Health System (MHS)
DITSCAP Checklist

Requirement	Description	Information Assurance Service
3.16 Access for Need-to-Know	Access to all DoD information is determined by both its classification and user need-to-know. Need-to-know is established by the Information Owner and enforced by discretionary or role-based access controls. Access controls are established and enforced for all shared or networked file systems and internal websites, whether classified, sensitive, or unclassified. All internal classified, sensitive, and unclassified websites are organized to provide at least three distinct levels of access: (1) Open access to general information that is made available to all DoD authorized users with network access. Access does not require an audit transaction. (**Ref:** DoDI 8500.2, February 6, 2003)	**Confidentiality**
	(2) Controlled access to information that is made available to all DoD authorized users upon the presentation of an individual authenticator. Access is recorded in an audit transaction. (3) Restricted access to need-to-know information that is made available only to an authorized community of interest. Authorized users must present an individual authenticator and have either a demonstrated or validated need-to-know. All access to need-to-know information and all failed access attempts are recorded in audit transactions. (**Ref:** DoDI 8500.2, February 6, 2003)	**Confidentiality**
3.17 Audit Record Content	Audit records include: - User ID. - Successful and unsuccessful attempts to access security files. - Date and time of the event. - Type of event. - Success or failure of event. - Successful and unsuccessful logons. - Denial of access resulting from excessive number of logon attempts. - Blocking or blacklisting a user ID, terminal or access port and the reason for the action. - Activities that might modify, bypass, or negate safeguards controlled by the system. (**Ref:** DoDI 8500.2, February 6, 2003)	**Confidentiality**
3.19 Encryption for Confidentiality (Data at Rest)	If required by the information owner, NIST-certified cryptography is used to encrypt stored sensitive information. (**Ref:** DoDI 8500.2, February 6, 2003)	**Confidentiality**
3.20 Encryption for Confidentiality (Data in Transit)	Unclassified, sensitive data transmitted through a commercial or wireless network are encrypted using NIST-certified cryptography (See also DCSR-2). (**Ref:** DoDI 8500.2, February 6, 2003)	**Confidentiality**

Military Health System (MHS)
DITSCAP Checklist

Requirement	Description	Information Assurance Service
3.21 Interconnections among DoD Systems and Enclaves	Discretionary access controls are a sufficient IA mechanism for connecting DoD information systems operating at the same classification, but with different need-to-know access rules. A controlled interface is required for interconnections among DoD information systems operating at different classifications levels or between DoD and non-DoD systems or networks. Controlled interfaces are addressed in separate guidance. (**Ref:** DoDI 8500.2, February 6, 2003)	**Confidentiality**
3.22 Logon	Successive logon attempts are controlled using one or more of the following: - access is denied after multiple unsuccessful logon attempts. - the number of access attempts in a given period is limited. - a time-delay control system is employed. If the system allows for multiple-logon sessions for each user ID, the system provides a capability to control the number of logon sessions. (**Ref:** DoDI 8500.2, February 6, 2003)	**Confidentiality**
3.23 Least Privilege	Access procedures enforce the principles of separation of duties and "least privilege." Access to privileged accounts is limited to privileged users. Use of privileged accounts is limited to privileged functions; that is, privileged users use non-privileged accounts for all non-privileged functions. This control is in addition to an appropriate security clearance and need-to-know authorization. (**Ref:** DoDI 8500.2, February 6, 2003)	**Confidentiality**
3.24 Marking and Labeling	Information and DoD information systems that store, process, transit, or display data in any form or format that is not approved for public release comply with all requirements for marking and labeling contained in policy and guidance documents, such as DOD 5200.1R. Markings and labels clearly reflect the classification or sensitivity level, if applicable, and any special dissemination, handling, or distribution instructions. (**Ref:** DoDI 8500.2, February 6, 2003)	**Confidentiality**
3.25 Conformance Monitoring and Testing	Conformance testing that includes periodic, unannounced, in-depth monitoring and provides for specific penetration testing to ensure compliance with all vulnerability mitigation procedures such as the DoD IAVA or other DoD IA practices is planned, scheduled, and conducted. Testing is intended to ensure that the system's IA capabilities continue to provide adequate assurance against constantly evolving threats and vulnerabilities. (**Ref:** DoDI 8500.2, February 6, 2003)	**Confidentiality**

Military Health System (MHS)
DITSCAP Checklist

Requirement	Description	Information Assurance Service
3.26 Encryption for Need-To-Know	Information in transit through a network at the same classification level, but which must be separated for need-to-know reasons, is encrypted, at a minimum, with NIST-certified cryptography. This is in addition to ECCT (encryption for confidentiality). (**Ref:** DoDI 8500.2, February 6, 2003)	**Confidentiality**
3.27 Resource Control	All authorizations to the information contained within an object are revoked prior to initial assignment, allocation, or reallocation to a subject from the system's pool of unused objects. No information, including encrypted representations of information, produced by a prior subject's actions is available to any subject that obtains access to an object that has been released back to the system. There is absolutely no residual data from the former object. (**Ref:** DoDI 8500.2, February 6, 2003)	**Confidentiality**
3.28 Audit Record Retention	If the DoD information system contains sources and methods intelligence (SAMI), then audit records are retained for 5 years. Otherwise, audit records are retained for at least 1 year. (**Ref:** DoDI 8500.2, February 6, 2003)	**Integrity**
3.29 Tempest Controls	Measures to protect against compromising emanations have been implemented according to DoD Directive S-5200.19. (**Ref:** DoDI 8500.2, February 6, 2003)	**Confidentiality**
3.30 Warning Message	All users are warned that they are entering a Government information system, and are provided with appropriate privacy and security notices to include statements informing them that they are subject to monitoring, recording and auditing. (**Ref:** DoDI 8500.2, February 6, 2003)	**Confidentiality**
3.31 Account Control	A comprehensive account management process is implemented to ensure that only authorized users can gain access to workstations, applications, and networks and that individual accounts designated as inactive, suspended, or terminated are promptly deactivated. (**Ref:** DoDI 8500.2, February 6, 2003)	**Confidentiality**
4.0 Enclave Boundary Defense		
4.1 Boundary Defense	Boundary defense mechanisms to include firewalls and network intrusion detection systems (IDS) are deployed at the enclave boundary to the wide area network, at layered or internal enclave boundaries and at key points in the network, as required. All Internet access is proxied through Internet access points that are under the management and control of the enclave and are isolated from other DoD information systems by physical or technical means. (**Ref:** DoDI 8500.2, February 6, 2003)	**Confidentiality**
4.2 Connection Rules	The DoD information system is compliant with established DoD connection rules and approval processes. (**Ref:** DoDI 8500.2, February 6, 2003)	**Availability**

Requirement	Description	Information Assurance Service
4.3 Virtual Private Network Controls (VPN)	All VPN traffic is visible to network intrusion detection systems (IDS). (**Ref:** DoDI 8500.2, February 6, 2003)	**Availability**
4.4 Intrusion Detection	Certify and evaluate the availability and effectiveness of tools and procedures to ensure real-time monitoring and alerts, intrusion detection, network analysis, audit analysis, user management, risk analysis, and network configuration management tools. (**Ref:** DoD 8510.1-M, July 2000).	**Availability**
4.5 Public WAN Connection	Connections between DoD enclaves and the Internet or other public or commercial wide area networks require a demilitarized zone (DMZ). (**Ref:** DoDI 8500.2, February 6, 2003)	**Confidentiality**
4.3 Remote Access for Privileged Functions	Remote access for privileged functions is discouraged, is permitted only for compelling operational needs, and is strictly controlled. In addition to EBRU-1, sessions employ security measures, such as a VPN with blocking mode enabled. A complete audit trail of each remote session is recorded, and the IAM/O reviews the log for every remote session. (**Ref:** DoDI 8500.2, February 6, 2003)	**Confidentiality**
4.4 Remote Access for User Functions	All remote access to DoD information systems, to include telework access, is mediated through a managed access control point, such as a remote access server in a DMZ. Remote access always uses encryption to protect the confidentiality of the session. The session level encryption equals or exceeds the robustness established in ECCT. Authenticators are restricted to those that offer strong protection against spoofing. Information regarding remote access mechanisms (e.g., Internet address, dial-up connection telephone number) is protected. (Ref: DoDI 8500.2, February 6, 2003)	**Confidentiality**
5.0 Continuity		
5.1 Alternate Site Designation	An alternate site is identified that permits the partial restoration of mission or business essential functions. (**Ref:** DoDI 8500.2, February 6, 2003)	**Availability**
5.2 Protection of Backup and Restoration Assets	Procedures are in place assure the appropriate physical and technical protection of the backup and restoration hardware, firmware, and software, such as router tables, compilers, and other security-related system software. (**Ref:** DoDI 8500.2, February 6, 2003)	**Availability**
5.3 Data Backup Procedures	Data backup is performed at least weekly. (**Ref:** DoDI 8500.2, February 6, 2003)	**Availability**

Military Health System (MHS)
DITSCAP Checklist

Requirement	Description	Information Assurance Service
5.3.1 Data Continuity	Certify that each file or data collection in the system has an identifiable source throughout its life cycle. (**Ref:** OMB A-130, Appx III, Transmittal No. 4)	**Availability**
5.4 Disaster and Recovery Planning	A disaster plan exists that provides for the partial resumption of mission or business essential functions within 5 days of activation. (Disaster recovery procedures include business recovery plans, system contingency plans, facility disaster recovery plans, and plan acceptance.) (**Ref:** DoDI 8500.2, February 6, 2003)	**Availability**
5.5 Enclave Boundary Defense	Enclave boundary defense at the alternate site provides security measures equivalent to the primary site. (**Ref:** DoDI 8500.2, February 6, 2003)	**Availability**
5.6 Scheduled Exercises and Drills	The continuity of operations or disaster recovery plans are exercised annually. (**Ref:** DoDI 8500.2, February 6, 2003)	**Availability**
5.7 Identification of Essential Functions	Mission and business essential functions are identified for priority restoration planning. (**Ref:** DoDI 8500.2, February 6, 2003)	**Availability**
5.8 Maintenance Support	Maintenance support for key IT assets is available to respond within 24 hours of failure. (**Ref:** DoDI 8500.2, February 6, 2003)	**Availability**
5.9 Power Supply	Electrical power is restored to key IT assets by manually activated power generators upon loss of electrical power from the primary source. (**Ref:** DoDI 8500.2, February 6, 2003)	**Availability**
5.10 Spares and Parts	Maintenance spares and spare parts for key IT assets can be obtained within 24 hours of failure. (**Ref:** DoDI 8500.2, February 6, 2003)	**Availability**
5.11 Backup Copies of Critical SW	Back-up copies of the operating system and other critical software are stored in a fire rated container or otherwise not collocated with the operational software. (**Ref:** DoDI 8500.2, February 6, 2003)	**Availability**
5.12 Trusted Recovery	Recovery procedures and technical system features exist to ensure that recovery is done in a secure and verifiable manner. Circumstances that can inhibit a trusted recovery are documented and appropriate mitigating procedures have been put in place. (**Ref:** DoDI 8500.2, February 6, 2003)	**Availability**
6.0 Vulnerability and Incident Management		
6.1 Incident Response Planning	An incident response plan exists that identifies the responsible Computer Network Defense Service Provider in accordance with DoD Instruction O-8530.2, defines reportable incidents, outlines a standard operating procedure for incident response to include INFOCON, provides for user training, and establishes an incident response team. The plan is exercised at least annually. (**Ref:** DoDI 8500.2, February 6, 2003)	**Availability**

Military Health System (MHS)
DITSCAP Checklist

Requirement	Description	Information Assurance Service
6.2 Vulnerability Management	A comprehensive vulnerability management process that includes the systematic identification and mitigation of software and hardware vulnerabilities is in place. Wherever system capabilities permit, mitigation is independently validated through inspection and automated vulnerability assessment or state management tools. Vulnerability assessment tools have been acquired, personnel have been appropriately trained, procedures have been developed, and regular internal and external assessments are conducted. For improved interoperability, preference is given to tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and use the Open Vulnerability Assessment Language (OVAL) to test for the presence of vulnerabilities. (**Ref:** DoDI 8500.2, February 6, 2003)	**Availability**
6.3 Assurance	Each information system shall be accredited to operated in accordance with a DAA-approved set of security safeguards. Accreditation will provide the DAA with a measure of confidence that the security features and architecture of an information system accurately mediates and enforces the security policy. (**Ref:** DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Directive & Instruction, 5200.40, December 1997and DoD 8510.1-M, July 2000)	**Availability**
6.4 Interim Approval To Operate (IATO)	Information system may be granted and Interim Approval To Operate (IATO) in accordance with a DAA-approved set of security safeguards. The IATO will allow the information system to deploy while enhancement to the security posture of the information system are being implemented. (**Ref:** DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Directive & Instruction, 5200.40, December 1997and DoD 8510.1-M, July 2000)	**Availability**
6.5 Approval to Operate (ATO)	Each information system shall be accredited to operated in accordance with a DAA-approved set of security safeguards. Accreditation will provide the DAA with a measure of confidence that the security features and architecture of an information system accurately mediates and enforces the security policy. (**Ref:** DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Directive & Instruction, 5200.40, December 1997and DoD 8510.1-M, July 2000)	**Availability**

Military Health System (MHS)
DITSCAP Checklist

Requirement	Description	Information Assurance Service
6.6 System Security Periodic Reviews	Information system shall be subject to system security periodic reviews to ensure no new security risk to the information system has been introduced since the receipt of an ATO for the information system. The periodic reviews will also validate that any changes to the information system since the receipt of an ATO are properly documented. (**Ref:** DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Directive & Instruction, 5200.40, December 1997and DoD 8510.1-M, July 2000)	**Availability**
6.7 Re-Accreditation	Each information system shall be accredited to operated in accordance with a DAA-approved set of security safeguards. Accreditation will provide the DAA with a measure of confidence that the security features and architecture of an information system accurately mediates and enforces the security policy. (**Ref:** DoD Information Technology Security Certification and Accreditation Process (DITSCAP) Directive & Instruction, 5200.40, December 1997and DoD 8510.1-M, July 2000)	**Availability**

Term	Definition
Availability	Timely, reliable access to data and information services for authorized users.
Confidentiality	Assurance that information is not disclosed to unauthorized entities or processes.
Integrity	Quality of an information system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the protection mechanisms; and the consistency of the data structures and occurrence of the stored data. Note that, in a formal security mode, integrity is interpreted more narrowly to mean protection against unauthorized modification or destruction of information.